COMMONWEALTH OF MASSACHUSETTS
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department of Telecommunications and Energy on its own Motion pursuant to G.L. c. 159, §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	DTE 02-8

PANEL REBUTTAL TESTIMONY OF

AT&T COMMUNICATIONS OF NEW ENGLAND, INC.

Michael Paszynsky
Anthony Fea
Douglas Gorham
E. Christopher Nurse

PUBLIC VERSION

May 15, 2002

I. QUALIFICATIONS AND STATEMENT OF PURPOSE

Q: PLEASE STATE THE NAME AND BUSINESS ADDRESS OF THE INDIVIDUAL PANEL MEMBERS TESTIFYING ON BEHALF OF AT&T COMMUNICATIONS OF NEW ENGLAND, INC. ("AT&T").

A: The members of the panel are Michael Paszynsky, Anthony Fea, Douglas Gorham and Christopher Nurse. Mr. Paszynsky's business address is 55 Corporate Drive, Bridgewater, New Jersey. Mr. Fea's business address is 429 Ridge Road, Dayton, New Jersey. Mr. Gorham's business address is 19 Brigham Street, Marlborough, Massachusetts. Mr. Nurse's business address is 3033 Chain Bridge Road, Oakton, Virginia.

Q: PLEASE STATE THE CURRENT POSITION, EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE OF EACH PANEL MEMBER.

A: **Mr. Michael Paszynsky** is the Director of Corporate Security & Claims for AT&T, the highest-ranking security professional in the corporation. He has been with AT&T Corporate Security for some 25 years in various positions, one of them being the Physical Security Staff Manager for the entire corporation. Amongst his current responsibilities, which include emergency planning and crisis management, he also teaches physical security at AT&T's in-house courses, such as Basic Investigator Training (BITS). Mr. Paszynsky is a graduate of the John Jay College of Criminal Justice (City University of New York) with a B.A. in Criminal Justice. He is also a Certified Protection Professional (CPP). Prior to joining AT&T, Mr. Paszynsky developed extensive experience with complex security designs as a Criminal Investigation Division (CID) Special Agent in the U.S. Army Reserve. He graduated from the Army's CID Academy and its Physical Security School. Mr. Paszynsky is currently a Board of Directors Nominee for the

International Security Management Association (ISMA) and a member in good standing of the American Society for Industrial Security (ASIS), National Association of Certified Fraud Examiners (NACFE), and the International Association of Chiefs of Police (IACP).

Mr. Anthony Fea is a Division Manager with AT&T Local Network Services, the organization within AT&T Corp. that provides local service (either entirely or partially through the use of AT&T's own facilities) to AT&T business customers of all sizes. Among other responsibilities, Mr. Fea oversees the planning of AT&T's local optical network in the northeastern part of the United States. Mr. Fea also assists in the development of a capital investment plan which optimizes the use of limited capital dollars, while at the same time appropriately controlling expenses and allowing for a return on the company's investment. Mr. Fea is a 1986 graduate of Stevens Institute of Technology, with a B.S. in Electrical Engineering. Since obtaining his degree, Mr. Fea has worked at a number of telecommunications firms including Bell Atlantic (now Verizon), Telecordia Technologies (BellCore), and most recently TCG and AT&T. Mr. Fea has previously testified before the Department in DTE 01-31, the Department's review of Verizon's proposal for Alternative Regulation.

Mr. Douglas Gorham is the Operations Manager with AT&T Local Network Services ("ALNS") for Massachusetts, New Hampshire and Maine. Part of his duties in this role is to coordinate, maintain and ensure AT&T operating standards at ALNS facilities. Mr. Gorham has been involved with the design, build out and operational procedures of nodes and collocation cages since 1993. He is familiar with many Verizon-Massachusetts Central Offices where AT&T has collocation arrangements, and

the current Verizon procedures CLECs must follow to gain access to their collocated facilities. Mr. Gorham received an A.S. in Electrical Engineering and a B.S. in Electronics Engineering from Wentworth Institute of Technology. He has been in the telecommunications industry for the last 9 years with Teleport and AT&T.

Mr. E. Christopher Nurse is District Manager of Government Affairs for AT&T Corp. He received his B.A. in Economics from the University of Massachusetts at Amherst and a Masters in Business Administration from Southern New Hampshire University in Manchester, New Hampshire. Prior to the promotion to his current position, Mr. Nurse was Manager of Government Affairs, and Manager of Regulatory and External Affairs for AT&T Local Services. Before joining AT&T, Mr. Nurse was employed in the same capacity by Teleport Communications Group Inc. Mr. Nurse was also a Telecommunications Analyst with the New Hampshire Public Utilities Commission from 1991 to 1997. Assigned to the Engineering Department, he was a lead analyst or a contributing analyst to nearly all telecommunications dockets before that Commission. In addition to dealing extensively with collocation matters, Mr. Nurse has extensive experience in metrics and remedies and is a regular member of the Carrier Working Group under the auspices of the New York Public Service Commission.

Q: PLEASE STATE THE PURPOSE OF YOUR TESTIMONY.

A: The purpose of this testimony is to address the issues that the Department raised in the notice it issued opening this investigation. In its notice, the Department stated:

> This investigation will determine whether Verizon's security policies meet the statutory standard for "just, reasonable, safe, adequate and proper regulations and practices." G.L. c. 159, § 16. Specifically, this investigation will include, but not be limited to, an examination of the following issues: (1) the extent and nature of appropriate access by personnel of other carriers to Verizon's central offices and other facilities for accessing collocation sites; (2) whether cageless collocation arrangements remain an acceptable security risk; (3) the adequacy of security

measures implemented in Verizon's central offices and other facilities, focusing on preventive, rather than "after-the-fact," measures; and (4) any other related security issues.

Notice of Investigation and Public Hearing (January 24, 2002) ("*Notice*"), at 1.

II. METHOD FOR ADDRESSING ISSUES RAISED BY THE DEPARTMENT IN ITS NOTICE.

Q. HOW SHOULD THE DEPARTMENT APPROACH THE PROBLEM OF DETERMINING WHAT TYPES OF COLLOCATION REGULATIONS AND PRACTICES ARE "JUST, REASONABLE, SAFE, ADEQUATE AND PROPER" IN LIGHT OF SECURITY ISSUES THAT HAVE ARISEN SINCE THE DEPARTMENT ESTABLISHED THE EXISTING COLLOCATION REGULATIONS AND PRACTICES?

A. AT&T is aware that the Department has previously ruled on and required Verizon to implement many of the existing collocation arrangements. AT&T understands that, when the Department made those rulings, it took into account all appropriate operational, competitive, and security concerns then known and understood, as well as the rules of the Federal Communications Commission governing collocation arrangements. AT&T also understands that the Department wants to revisit those rulings to determine whether there is a need to change what has previously been determined to be appropriate collocation security arrangements in light of security issues that have since arisen. The issues that the Department has raised in this proceeding, therefore, are limited: What has changed since the Department's prior rulings? What security issues need to be addressed that were not addressed in the Department's prior rulings? And, most importantly, how much security is enough security; that is, what criteria should we use to determine how much security is enough security?

Q. WHAT DO YOU MEAN BY "HOW MUCH SECURITY IS ENOUGH SECURITY"?

A. It is, of course, always possible to increase the level of security. However, increasing levels of security come with increasing costs -- both visible costs, such as new construction and equipment costs, and less visible costs, such as operational inefficiencies and impairment of competition.

Any security plan must recognize the expense and inconvenience associated with certain measures. After analyzing the risks facing telecommunications facilities in Massachusetts, it is necessary to determine how much inconvenience is warranted and what level of cost is appropriate. It is necessary, therefore, to determine the point at which increasingly costly security measures provide such a small improvement to actual security, that it is no longer worth the cost. It is simply not possible to decide whether there is sufficient "security" in the abstract, because we can never achieve complete and perfect security.

Any determination of the appropriate type of collocation arrangements for achieving "adequate" security must necessarily balance the cost of changing the existing collocation arrangements (which were determined to be optimal prior to concerns raised by the September 11th terrorist attacks) against the benefits such increased security measures produce. Moreover, where increased security can be achieved through measures that do not involve significant changes to previously determined collocation arrangements and that do not interfere with important policy goals -- such as the development of competition -- those measures should be used instead of costly, anti-competitive alternatives.

When analyzing what, if any, new security measures are necessary, the Department should be mindful of the importance of proper security *procedures*. Experts estimate that upwards of 90% of all security failures are a result of procedural shortfalls rather than a failure or lack of security *devices*. It is AT&T's position that, in general, Verizon's central offices are currently equipped with physical security devices which are more than adequate to do the job. Assuming that improvements to central office security are found necessary, the Department's focus should be upon improving Verizon's policies and procedures while using the security technology already in the field. This is how real improvements in central office security are likely to be made.

It is important for the Department to remember that all security is based upon the "3-P Principle", i.e., **P**eople, **P**hysical security hardware/devices, and **P**olicies and procedures. Removing one of these elements results in a break in the security loop, creating the potential for security failures. The Department should train its focus upon the third element of the 3-P Principle -- policies and procedures -- in this proceeding.

Q. WHAT INFORMATION DOES THE DEPARTMENT NEED, THEN, TO DETERMINE WHETHER EXISTING COLLOCATION SECURITY ARRANGEMENTS ARE APPROPRIATE?

A. The Department needs to know what new risks are posed by collocation arrangements that were not apparent when it ordered its existing collocation rules. Understanding the gravity of these new risks requires measuring the likelihood of an adverse event and the magnitude and type of consequences that would result from such an event. Once the Department has some sense of the scale of the risks, it will need to investigate a range of security measures before it can determine whether changes in collocation rules are the least cost means of addressing the identified risk. Finally, since costs associated with any

change in collocation rules are ultimately borne by Massachusetts consumers, the Department will need information regarding the value of the security benefit before it can determine whether the costs associated with changing the collocation arrangements are warranted.

Q. IS AT&T ABLE TO PROVIDE THE INFORMATION THAT THE DEPARTMENT REQUIRES?

A. AT&T can provide some of the information. Some of the information that the Department needs, however, is information that Verizon ought to have, but has yet to provide to the Department.

Specifically, AT&T can provide information relating to the assessment of security risks. It can also describe the most cost effective means of addressing those risks in its experience. AT&T, however, cannot provide detailed information regarding the cost of alternative approaches to security that Verizon has proposed (*i.e.*, the costs of the substantial changes in collocation arrangements that Verizon proposes). That information needs to come from a couple of different sources. AT&T can provide information regarding the costly disruptions to AT&T's operations that would be caused by the collocation rule changes proposed by Verizon. That information is presented later in this testimony. The actual costs of construction, relocation of equipment, and alteration of physical plant that is called for by Verizon's proposal will need to come from Verizon. Based on my review of Verizon's testimony and discovery responses, it does not appear that Verizon has made any effort to estimate those costs.

Q. WILL YOU ALSO BE COMMENTING ON VERIZON'S TESTIMONY IN THIS PROCEEDING?

A. Yes. As part of its presentation of identifying risks and describing AT&T's experience in addressing those risks, AT&T will highlight the problems with Verizon's proposal. AT&T will also show that the risks that Verizon has identified are nothing new and that, in AT&T's experience, they can be addressed with far less costly measures than the changes in collocation rules that Verizon proposes.

III. RISK ASSESSMENT.

Q. WHAT NEW RISKS ARE PRESENTED THAT THE DEPARTMENT DID NOT CONSIDER WHEN IT DETERMINED THE EXISTING COLLOCATION RULES.

A. The new types of risks that security experts are now considering are unlikely to be the types of risks that collocation rules for telecommunications central offices can or should address. While an attack upon the physical integrity of telecommunications facilities is a security concern that should never be overlooked, the likelihood of such an attack is small in comparison to the likelihood of a remotely directed electronic or cyber attack. Such remotely directed attacks would accomplish the same damage to the telecommunications infrastructure as a physical attack – namely the disablement of central office equipment. Moreover, such remote attacks could be attempted by terrorist elements in a much more clandestine fashion, providing a greater opportunity for such elements to avoid capture by law enforcement.

Furthermore, terrorist organizations plotting a physical attack like those carried out on September 11th are more likely to focus their attention on other public utility systems such as water or energy facilities. Physical attacks upon such facilities would, generally speaking, have more profound and deadly effects upon the population, making

them a more attractive option for terrorists like those responsible for the events of September 11th. The destruction of a telephone central office would not have the far-reaching effect that an attack upon a nuclear power plant or dam system would, for instance.

To the extent that this proceeding has been initiated to examine risks not previously addressed when the existing collocation rules were put in place, there is little that an adjustment to these rules could accomplish. The new security risks that have materialized of late, namely organized terrorist threats, cannot be properly addressed through a change in collocation policy. AT&T understands, however, that the Department may want to reexamine collocation arrangements in any event to address already recognized risks.

Q. WHAT ARE THE TYPICAL TYPES OF RISKS THAT ARE RAISED IN THE CONTEXT OF COLLOCATION ARRANGEMENTS?

A. Verizon's testimony provides examples of certain security breaches that have occurred throughout the country. Although Verizon indicates that there have been occasional incidents across the country, including former GTE territory, Verizon's testimony provides absolutely no verifiable evidence of the extent of such occurrences. Thus, while Verizon has identified certain isolated incidents, it provides no data regarding the extent of the risk and therefore no evidence regarding the value or benefit that would be obtained by implementing measures needed to prevent such risks.

Verizon lists the following alleged incidents:

?? Unauthorized entry into central offices

?? Theft and vandalism of CLEC equipment resulting from unauthorized access to a CLEC's cage

?? Theft and vandalism of Verizon equipment in secured and unsecured areas of the central office

?? Cables cut on frames

?? CLEC entry into central offices without an authorized identification badge or electronic access card

?? CLEC entry into central offices with unauthorized use of another's identification badge or electronic access card

?? Central Office doors propped open or locks taped

?? Acts of vandalism such as broken locks on doors or collocation cages, card readers destroyed, or power systems disabled

?? Unauthorized CLEC testing on Verizon's side of the equipment

?? Claims of drug use on the central office premises

?? Other improper conduct (e.g., (1) CLEC entry into Verizon's BDFB causing a service outage in a remote switch, interrupting service to 9,000 customers and (2) breaking into locked power rooms.)

While the identification of certain incidents is of some use in analyzing proper security procedures, without data concerning the frequency of such events in Massachusetts, it is impossible to measure the value of Verizon's proposed additional security measures. And, certainly, several of the alleged incident types Verizon cites, such as drug use and CO doors propped open, are strongly suggestive of acts committed by those who have legitimate access to the premises. How then does Verizon exclude its own employees from suspicion?

IV. SECURITY MEASURES FOR THE RISKS IDENTIFIED.

Q. BASED ON AT&T'S EXPERIENCE, PLEASE DESCRIBE THE SECURITY MEASURES THAT ARE TYPICALLY USED TO CONTROL THE RISKS IDENTIFIED.

A. Although AT&T is not required to provide collocation space to other carriers, AT&T has space license arrangements in some of its central offices that result in the placement of third-party facilities in those offices. AT&T has large business and government customers as well as CLECs and ILECs, including Verizon, maintaining equipment in its buildings. AT&T previously provided to the DTE a summary of its security practices and it regards that document as being confidential. However, as a general proposition, physical access to AT&T's switching centers and other network facilities is strictly monitored and managed. AT&T has well-developed procedure for controlling access to its buildings, including many of the same security measures that Verizon states it uses.

Q. WHAT ARE THE SECURITY MEASURES THAT VERIZON MENTIONED IN ITS TESTIMONY?

A. According to pp. 16-17 of Verizon's testimony, Verizon currently uses the following security measures:

1. non-Verizon employee collocation identification cards
2. electronic card reader access systems
3. key controlled access systems
4. directional signage and floor markings (e.g., floor tape)
5. access through guarded entries.
6. security cameras (*i.e.*, Closed Circuit Television ("CCTV")) in COs with cageless collocation open environment ("CCOE")

Each measure is described in Attachment 1 to that testimony.

Q. IN AT&T'S EXPERIENCE, DO THESE TYPES OF SECURITY MEASURES ADDRESS THE RISKS THAT VERIZON HAS IDENTIFIED?

A. When used in combination with AT&T's other practices, these measures are more than adequate to reasonably ensure security.

Q. ARE YOU AWARE THAT VERIZON CLAIMS THAT THE SECURITY MEASURES DESCRIBED ON PP. 16-17 OF VERIZON'S TESTIMONY THAT BOTH AT&T AND VERIZON USE CAN'T POSSIBLY SOLVE THE PROBLEMS IT CITES?

A. Yes. On pages 17-21 of Verizon's testimony, Verizon argues that these security measures are not "preventative" and then provides superficial reasons why cameras and security access cards *each standing alone* will always be inadequate. It doesn't give any reasons why its other security measures will not work, and more importantly, it doesn't give any reason why all the security measures employed in combination cannot work.

In addition, on page 20, Verizon claims, in footnote 18, that "breaches [of its security protocols for using access cards] often go undetected and unpunished because Verizon does not have the same recourse against CLEC violators as it does with its own employees or vendors (*i.e.*, Verizon cannot discipline a CLEC violator or terminate his/her employment.)" Clearly, optimal security requires communication of alleged security breaches between resident companies' Security Organizations so that corrective action, including discipline, can be taken. Each company can certainly discipline its own employees following investigation of a breach.

Q. BASED ON YOUR EXPERIENCE WITH THE SECURITY MEASURES THAT VERIZON USES, DO YOU AGREE THAT THE "INADEQUACIES" OF THE SECURITY MEASURES THAT VERIZON DESCRIBES MEAN THAT ITS CURRENT SECURITY MEASURES CANNOT ADDRESS THE PROBLEMS IT HAS CITED?

A. Our answer is an emphatic "no."

First of all, as stated earlier, AT&T uses these same security measures in its own facilities. There are other carriers and customers located in our facilities, and we find that these security measures work well when properly implemented, properly administered, and used in combination.

Second, the reasons that Verizon gives for the alleged inadequacies of its current measures are not reasons that any reasonable security expert would use for rejecting a security measure in favor of far more expensive and impractical policy:

a. The claim that current measures are not preventative is not accurate. Every measure that makes the undesirable behavior to which it is targeted less likely is preventative. It's a matter of common sense that the presence of cameras, for example, will deter some portion of the undesirable conduct. Indeed, a common security measure is the installation of "dummy" cameras in order to make people think they are being watched. Or take, as another example, an access card reader. When individuals know that their presence can be traced back to a central office at a particular time, such knowledge acts as a deterrent to undesirable content.

b. The claim that cameras do not capture every angle and are not "real time" is not a reason to implement alternative, draconian measures. Cameras fitted with motion sensors, can, in fact, be set-up for real-time operation and viewing. Moreover, the ability of cameras to capture "every angle" is very much a function of how the cameras are positioned and how many cameras are deployed. The choice between

adding a few more cameras, on the one hand, and implementing costly and impractical collocation rules on the other should be driven by an evaluation of costs and benefits. Similarly, Verizon's claim that its current cameras are not "real time" is not, by itself, a justification for costly and cumbersome alternative measures. The more common sense approach is to address the specific concern. Many options exist in the case of security cameras. These can range from full motion video (15 frames per second) with motion sensors to the "dummy" cameras mentioned earlier. Excluding all carriers from their equipment or embarking upon the wholesale construction of separate entrances is not justified simply because Verizon does not currently use cameras effectively to monitor and prevent undesirable conduct.

c. The claim that access cards only provide a witness or suspect after the fact and do not show when an individual leaves is not accurate. As mentioned earlier, access cards can be an effective deterrent. Moreover, access systems come with various options. While some require swiping on entrance only, others require card swiping on entrance *and exit*. This is a feature know as "anti-passback". Some allow activation for certain periods of time based on the individual card. There are also high technology biometric devices that require authentication based on fingerprints or retinal scans. On the low end of the scale are key and/or combination locks. Again, the decision as to what type of access system to use needs to be based on the type of security risks and the potential impact of an incident. Furthermore, this is one piece of the overall security plan and would depend on the other pieces of the solution, such as, use of another system used

for logging in and out of a building; use of remotely operated doors in connection with a voice and video link; the number of employees and/or security guards on site, etc. Once again, however, it is important for the Department to remember that physical security devices are but one of three requisite elements to achieve true security. Competent people and appropriate security policies are more critical to providing effective security than any particular hardware.

d. Finally, the claim that breaches of security protocols by CLEC employees go unpunished because Verizon does not have the same recourse against CLEC violators as it does with its own employees or vendors does not make sense. Part of a successful security plan requires appropriate training for each person requiring access. This includes familiarization with the proper procedures to follow, as well as the consequences of not following those procedures. Consequences can range from revoking an individual's access authorization to the pressing of criminal trespass charges. AT&T establishes compliance with its security protocols as a condition of entry for every person requiring access to an AT&T central office, whether the individual is an AT&T employee or an employee of a vendor, customer, CLEC, or ILEC. There is certainly no reason why Verizon cannot do the same. Indeed, Verizon's current rules permit it to bar offending CLEC personnel from central offices through the deactivation or recovery of access key cards.

e. Verizon has a code of conduct similar to AT&T's. Verizon's employees are required to report problems under their own policies. If they are not complying with those policies, there is nothing AT&T and other CLECs can do. Education is

a bona-fide key here. Formal in-person training, combined with reinforcement tools such as the posting of notices in all central offices where collocation takes place, is a good idea.

Third, Verizon does not explain precisely how it implements its current security measures. If these measures are implemented properly, they will protect against the problems cited by Verizon.

V. COSTS OF THE EXTRAORDINARY COLLOCATION CHANGES PROPOSED BY VERIZON.

Q. WHAT ARE THE COSTS ASSOCIATED WITH THE COLLOCATION RULE CHANGES PROPOSED BY VERIZON?

A. As mentioned at the outset, there are two general types of costs that arise from making the collocation rule changes proposed by Verizon. One is the visible costs of construction and equipment relocation. Until Verizon provides the details associated with its proposal it is not possible to estimate those costs. The other costs are the costs of network operation disruption, the detrimental impact on competition, and the increased need for regulatory oversight that results from Verizon's proposal. Those costs are addressed below. Of course there is also the opportunity cost representing the better alternative use of increasingly scarce resources.

Q. WHAT TYPES OF EQUIPMENT DOES AT&T PLACE IN COLLOCATION ARRANGEMENTS IN VERIZON CENTRAL OFFICES AND WHAT TYPES OF SERVICES DOES AT&T SEEK TO PROVIDE WITH THESE FACILITIES?

A. Collocation is a critical part of AT&T's strategy of becoming a facilities-based provider of local business and residential services. Without physical collocation, AT&T would not be able to cost effectively operate and maintain the critical elements required in the

"last mile" connection to the customer. AT&T generally places SONET transport and DSL/DLC access equipment in a collocation cage to hand off a variety of DS-0 to OC-x based services that are connected to the network of an incumbent local exchange company (ILEC) such as Verizon to meet the service demands of our customers. In addition, infrastructure elements required to support and maintain this equipment are installed in ILEC collocation cages. These elements typically consist of racking, power, cross-connect panels, etc. AT&T generally tries to provision service across AT&T owned and operated facilities where it is technically and economically feasible. In addition, AT&T generally places its own equipment in collocation arrangements in ILEC central offices. Our objective is to provide end-to-end local and long-distance services to our customers over as much of our own network as technically feasible.

Q. WHY DOES AT&T CHOOSE PHYSICAL OVER VIRTUAL COLLOCATION?

A. Physical collocation is AT&T's generally preferred method of interconnection with an ILEC for a variety of reasons. First, physical collocation allows AT&T to control its own network facilities, thereby allowing AT&T flexibility in choosing how to manage and maintain its physical plant within the collocation site. In addition, physical collocation minimizes the inherent delays associated with virtual collocation since it typically does not require a collocation application every time network growth and rearrangements are required. Finally, it eliminates potential conflicts that may arise when an ILEC and AT&T are simultaneously trying to install or restore service in the same place, as was the case at the Verizon Manhattan West Street Central Office after the September 11th terrorist attack.

Other reasons include:

1. The ability to provide our customers with a higher quality of service;

2. Control of provisioning intervals and mean time to repair (MTTR);

3. The ability to reduce long lead times regarding pre-provisioning items such as space, power and cabling;

4. Eliminating the need to maintain equipment spares and cabinets at every ILEC virtual collocation;

5. Eliminating the need to pay for new ILEC technician training every time an already trained technician is moved to different assignment;

6. Eliminating collocation application delays and issues that arise as a result of application process;

7. Eliminating potential for billing errors associated with collocation applications.

Q. VERIZON HAS PROPOSED THAT IN CERTAIN "HIGH RISK" CENTRAL OFFICES, CLECS SHOULD BE REQUIRED TO CONVERT THEIR PHYSICAL COLLOCATION ARRANGEMENTS INTO VIRTUAL ARRANGEMENTS. DOES AT&T AGREE WITH THIS PROPOSAL?

A. No. First, we are advised by counsel that Verizon's proposal directly violates both the 1996 Telecommunications Act, as well as FCC rules implementing that law which required ILECs such as Verizon to provide physical collocation, except where precluded by space limitations or technical considerations. Second, Verizon's proposal is based on erroneous assumptions and a flawed conception of "high risk." Finally, the anti-competitive implications of the proposal are severe, and the changes that would be needed to implement Verizon's proposal would be grossly disproportionate to the of claimed risk.

This testimony has already discussed the nature of the most likely potential threats to the telecommunications network, the likelihood of physical attack scenarios, and the types of appropriate security measures that are already in place to guard against them. The primary terrorist threat facing telecommunications facilities comes from cyber or

electronic sabotage. Given this, it makes little sense to categorize certain central offices as facing a "high risk" of physical attack.

Furthermore, the proposal to have competitive carriers convert their physical collocations into virtual arrangements presumes that CLEC technicians pose a threat sufficient to justify the anti-competitive and costly implications of such a conversion. However, CLEC personnel are no more likely than Verizon personnel to engage in intentional acts of vandalism, damaging network facilities. Thus, Verizon's proposal amounts to unreasonable discrimination against CLEC personnel.

Q. YOU STATE THAT THE VERIZON PROPOSAL TO CONVERT PHYSICAL ARRANGEMENTS TO VIRTUAL ARRANGEMENTS WOULD VIOLATE THE TELECOMMUNICATIONS ACT AND EXISTING FCC RULES. PLEASE EXPLAIN.

A. We are advised by counsel that the 1996 Telecommunications Act and related FCC rules imposes certain obligations upon ILECs such as Verizon with respect to collocation. Specifically, Section 251(c)(6) of the 1996 Act requires physical collocation "at the premise of the local exchange carrier." Section 251(c)(6) of the Act permits only two exceptions to its physical collocation requirement – where an ILEC "demonstrates to the state commission that physical collocation is not practical for technical reasons or because of space limitations." The FCC's implementing regulations repeat the Act's technical and space limitation language. *See* 47 C.F.R. 51.323(l). Thus, technical or space limitations are the sole reasons an ILEC can refuse to provide physical collocation in a particular location.

Q. SHOULD PHYSICAL COLLOCATION TAKE INTO ACCOUNT SECURITY CONCERNS?

A. We are advised by counsel that the FCC's rules do permit an ILEC to implement *reasonable* security arrangements to protect its equipment, but the ILEC may not use security risks to circumvent their statutory requirement to provide physical collocation. As stated above, only technical or space constraints may prevent a collocating carrier from entering into a physical collocation arrangement with the ILEC. Indeed, the FCC's narrowly tailored regulations make this clear. These regulations prohibit an ILEC from implementing security arrangements that are more stringent than those used by the ILEC for their own employees or contractors. The rules also expressly state that ILECs must allow collocating carriers access to their equipment "24 hours a day, seven days a week, without requiring either a security escort of any kind or delaying a competitor's employees' entry into the incumbent LEC's premises." 47 C.F.R. § 51.323(i). The FCC also gives some examples of "reasonable security arrangements" – installing security cameras, requiring competitive LEC personnel to use badges, or undergo the same level of security training as the ILECs' own employees or contractors. 47 C.F.R. § 51.323(i). Verizon's proposal in this proceeding is a far cry from what the FCC considers to be *reasonable* security measures.

Verizon's unsubstantiated concerns regarding security risks associated with certain central offices and the associated need to preclude physical interconnection at those locations clearly do not fall within either the technical feasibility or space limitation standards established by the Act, the FCC's implementing rules, or the FCC's narrowly tailored security standards. Although a state may adopt its own collocation requirements, those requirements must be consistent with the Act and FCC regulations.

Since Verizon's proposal relating to converting physical collocation to virtual collocation is not consistent with the Act or the FCC regulations, the Department may not adopt it.

Q. WHY IS VERIZON'S PROPOSAL TO CONVERT PHYSICAL COLLOCATIONS INTO VIRTUAL ARRANGEMENTS ANTI-COMPETITIVE FROM A BUSINESS PERSPECTIVE?

A. As Verizon has explained, virtual collocation is an arrangement in which "the CLEC leases its equipment to Verizon-MA to install, maintain, upgrade, and repair." In the most basic sense, virtual collocation is distinguished from physical collocation in that there is no locked cage surrounding and separating CLEC facilities from the other facilities and equipment in the central office. As Verizon states, "Unlike physical collocation, a virtual collocation arrangement does not require Verizon-MA to assign a portion of the floor space in the CO to the collocated carrier for its exclusive use to install, operate, and maintain its own equipment."

It is both inconsistent and unfair for Verizon to suggest that their central office equipment should be completely sealed off from any possibility of access by CLEC technicians, while at the same time, arguing that CLECs should be forced to turn over all access to, and responsibility for, their collocated facilities to Verizon. Indeed, a primary reason that AT&T incurs the significant expense associated with physical collocation cages is to be able to control access to our facilities and to provide additional security for our equipment. As discussed above, there is no evidence or reason to believe that Verizon personnel are any more, or less, trustworthy than CLEC personnel. It is inconsistent for Verizon to expect CLECs to expose their facilities to a level of risk that Verizon itself is unwilling to accept.

Additionally, AT&T purchases costly physical collocation arrangements in order to maintain control over the installation and maintenance of our collocated facilities. If AT&T has a new customer or immediate need for additional collocated equipment, it has the ability to expedite the installation of equipment to quickly meet that demand. Similarly, if there is a problem with our collocated equipment, we can ensure that it is immediately repaired. In this way, AT&T, and not Verizon, maintains control over our service quality. The competitive importance of this cannot be overstated. This control over our equipment, our timely delivery of service, and our service quality would be lost if the Department required AT&T to convert its physical collocation arrangements into virtual collocation arrangements.

Q. ARE THERE OTHER COMPETITIVE ISSUES PRESENTED BY VERIZON'S PROPOSAL TO FORCE CLECS TO USE VIRTUAL COLLOCATION?

A. Yes. As suggested above, a whole new array of ILEC performance issues come into play under Verizon's proposal for mandatory virtual collocation in certain COs. Under this proposal, in the event of an attack or act of vandalism that would affect both Verizon and CLEC facilities and customers, there are no guarantees that CLEC customers will be restored as quickly as Verizon's. Indeed, Verizon would have every incentive to restore the services of its own customers before turning to the repair of CLEC facilities. In the event of a service disruption, even something as simple as Verizon's familiarity with its own equipment and facilities, and lack of familiarity with CLEC facilities, would dictate that they, would be able to work or, would work on their equipment first to restore the largest number of customers in the shortest amount of time. The pool of highly skilled technicians available to expeditiously restore service would be reduced under Verizon

proposal which would exclude otherwise available CLEC technicians. The interests of smaller competitors and their end users could be lost in this environment.

In a more routine but equally important context, requiring CLECs to use virtual arrangements would raise the same types of "Type 2" provisioning and maintenance issues and problems that the Department is currently investigating with respect to Verizon's special access performance. CLECs would again be at the mercy of Verizon's ability and willingness to meet yet to be established intervals for the installation and maintenance of collocated CLEC equipment. We are advised by counsel that the FCC's rules require that an ILEC that provides virtual collocation must, at a minimum, install, maintain and repair collocated equipment within the same time period and with failure rates that are no greater than those that apply to the performance of similar functions for comparable equipment of the ILEC itself. *See* 47 C.F.R. 51.323(e). The only way the Department could ensure that Verizon complied with this rule would be to create an additional set of performance metrics, penalties, and reporting requirements – resulting in a significant and unnecessary regulatory and administrative burden for the Department and telecommunications providers. Even then, AT&T would have no assurance that Verizon's performance would meet the service quality standards that we provide our retail customers.

Q. WHAT IMPACT DOES VERIZON'S PROPOSAL FOR MANDATORY VIRTUAL COLLOCATION HAVE ON THE DEVELOPMENT OF "FACILITIES-BASED" COMPETITION?

A. Verizon's proposal would significantly undermine the development of facilities-based competition in areas of Massachusetts that are served by central offices that Verizon would designate as being of "high risk." AT&T notes that the Department has been a

long-time proponent of local competition, and in particular, of facilities-based competition. A policy that requires facilities-based carriers to cede the installation and maintenance of their equipment to Verizon would significantly undercut the entire notion of what it means to be "facilities-based." As stated above, CLECs would be unable to distinguish themselves from the ILEC by providing their customers with superior installation, maintenance or repair operations or services. Instead, they would be limited to those standards or service intervals that Verizon provides for its own customers. Moreover, requiring mandatory virtual collocation at certain sites would also create a disincentive for CLECs to purchase their own facilities at those sites. CLECs certainly would not build their own facilities at such sites only to turn them over to Verizon's control.

Q. HOW DOES VERIZON'S PROPOSAL IMPACT CLEC OPERATIONS FROM THE PERSPECTIVE OF NETWORK PLANNING?

A. AT&T's network planning and engineering has always taken security needs into consideration. From an engineering and growth planning perspective, however, Verizon's proposal would have important implications for AT&T's ability to serve its customers. In addition to the problems discussed above with respect to virtual collocation, AT&T has concerns with other several other aspects of Verizon's proposal.

Q. ONE ASPECT OF VERIZON'S PROPOSAL WOULD REQUIRE THE ESTABLISHMENT OF SEPARATE SPACE INCLUDING SEPARATE ENTRANCES AND OR PATHWAYS TO COLLOCATORS' EQUIPMENT, WHICH WOULD BE SEGREGATED FROM VERIZON'S EQUIPMENT. CAN YOU COMMENT ON THIS?

A. Yes. As noted in the above, the FCC rules allow ILECs to implement only reasonable security arrangements to protect its equipment and ensure network reliability. As noted previously, Verizon's current security measures, when implemented properly, adequately address the central office security risks. Any additional measures, especially ones with implications as onerous as those proposed by Verizon, are not reasonable and therefore should be rejected.

In addition, we are advised by counsel that any proposal for space separation must meet more stringent requirements under the FCC's regulations than other security arrangements. Specifically, the FCC rules indicate that restricting physical collocation to space separated from the space housing ILEC equipment must meet several conditions. Among other requirements, physical separation must be warranted by legitimate security concerns or operational constraints unrelated to the ILEC's competitive concerns. Verizon has not suggested that its proposal is associated with any operational constraints and, as demonstrated above, security concerns do not warrant any separation measures.

In addition, the FCC rules indicate that any construction of separate entrances must be technically feasible; must be related to legitimate security concerns or operational constraints; and must not artificially delay collocation provisioning or materially increase the requesting carriers costs. Since Verizon's proposal does not address any of the FCC's separation requirements, it has also not demonstrated that its proposal is consistent with FCC regulations.

Q. YOU MENTIONED THAT THESE SEPARATION REQUIREMENTS WOULD HAVE ONEROUS IMPLICATIONS. CAN YOU EXPLAIN HOW THESE SEPARATION PROPOSALS WOULD IMPACT AT&T'S NETWORK OPERATIONS?

A. Verizon's proposal would be very difficult and costly to implement and would ultimately reduce the amount of space available to CLECs for collocation in Verizon central offices. It has generally been Verizon's policy to designate specific areas in central offices as available to CLECs for collocation. In this respect, most CLEC equipment is already located in the same general area of a central office. However, the reconfiguration and necessary construction in each Verizon central office to allow for separate entrances and pathways is not likely to be feasible in many instances due to zoning, set back and other municipal regulations.

Verizon's proposal would most likely require CLECs to relocate their facilities and cages within Verizon central offices. This relocation process would be extremely costly and disruptive. For example, in order to relocate a CLEC's facilities without service disruption, it would be necessary to install parallel facilities in the new location, test those new facilities, and then migrate the CLEC's customers to those new facilities. This complex process requires significant labor and precise coordination and execution in order to avoid customer disruptions. Moreover, despite best efforts, it is more likely than not that customers will be affected and CLECs could lose customers as a result of the inevitable disruptions.

In addition, the migration process results in stranded investment in the old equipment in the abandoned collocation areas that would no longer be used. In addition to the investment being stranded, this actual equipment would also have to be removed. Clearly, the minimal amount of additional security provided by facility separation would

not be worth the man-hours, costs, and customer disruption associated with such conversions.

Q. VERIZON ALSO PROPOSES THE RELOCATION OF EXISTING UNSECURED CAGELESS COLLOCATION ARRANGEMENTS TO SEGREGATED AREAS OF CENTRAL OFFICES, OR THE CONVERSION OF THE ARRANGEMENTS TO VIRTUAL COLLOCATIONS WHERE SECURED SPACE IS UNAVAILABLE. IS THIS PROPOSAL WORKABLE?

A. No, for the reasons discussed previously, it is not. The relocation problems described above, such as frequent service disruptions and burdensome costs would exist here, as well. Whether the environment is one of physical collocation or cageless collocation, the problems and costs associated with a mass relocation of facilities will have a significant impact on CLECs' operations and services. Verizon's proposal for the conversion of cageless collocations to virtual is also unacceptable for the same reasons described in the earlier testimony concerning Verizon's proposed "high risk" central offices.

Q. VERIZON ALSO PROPOSES THAT CLEC ACCESS TO "SHARED FACILITIES," SUCH AS LOADING DOCKS, STAGING AREAS, AND RESTROOMS BE RESTRICTED OR LIMITED BY PARTITIONING VERIZON EQUIPMENT OR BY REQUIRING ESCORTS AT CLEC EXPENSE. DOES AT&T AGREE WITH THIS ASPECT OF THE PROPOSAL?

A. Once again, it is AT&T's opinion that such measures are not necessary to address security concerns at central offices. Verizon's current measures, when implemented properly, are adequate and effective to address the existing level of risk. Should Verizon want to implement the additional measures it proposes, however, it should assume the cost of those measures. The cost of erecting partitions to sequester Verizon's own equipment should be borne solely by Verizon since its policies would be the sole cause of that cost.

Verizon's assumption of this expense is also consistent with FCC rules that provide that CLECs need only pay for the least expensive, effective, and reasonable security option that is viable for the space assigned. *See* 47 C.F.R. 51.323(i). Since Verizon's proposed partitioning is not reasonably required, and is not the least expensive, yet effective security option, CLECs should not be required to pay for them under FCC regulations.

Verizon's partitioning of its own equipment would not, like Verizon's other proposals, adversely affect CLEC's operations and therefore AT&T does not oppose such measures, so long as Verizon assumes the concomitant expenses.

Q. PLEASE COMMENT UPON VERIZON'S PROPOSAL TO REQUIRE ESCORTS IN THE SHARED FACILITIES AREAS.

A. AT&T strongly opposes the proposal to require escorts to accompany CLEC technicians to and from "shared facilities." First, requiring escorts is explicitly precluded by FCC rules. The rules state that an ILEC must allow collocating parties to access their collocated equipment 24 hours a day, 7 days a week without requiring either a security escort of any kind or delaying a competitor's entry into the ILECs premises. *See* 47 C.F.R. 51.323(i). Verizon's proposal can result in both restricted access for CLECs to their own equipment as well as a general delayed entry into parts of the ILEC premise.

Moreover, escorts are impracticable since they result in both increased costs and delay associated with arranging an escort meeting. Consequently, AT&T's installation and repair metrics would be adversely impacted by this proposal.

Q. VERIZON HAS PROPOSED THAT EITHER VIRTUAL COLLOCATION OR ESCORTS BE REQUIRED AT REMOTE TERMINAL (RT) SITES. DO YOU AGREE?

A. No. Again, escorts are not necessary from the standpoint of security, nor are they permissible under current FCC rules. Additionally, for the reasons discussed at some length above, CLECs cannot not be forced into virtual collocation arrangements unless there are space or technical limitations. This rule applies both to Verizon's central offices as well as remote terminals. The FCC has found that the obligation to provide physical collocation at ILEC "premises" extends to not only central offices but to "serving wire centers, tandem offices as well as all buildings or similar structures owned or leased by the incumbent LEC that house LEC network facilities" and "any structures that house LEC network facilities on public rights of way, such as vaults containing loop concentrators or similar structures." *FCC's First Local Competition Order* at ¶ 573. Remote Terminals clearly fall within this broad definition.

Moreover, remote terminals generally house a very small fraction of the equipment that is found in a central office. Thus, imposing an escort requirement on these types of premises is completely unsupportable. This aspect of Verizon's proposal appears to be more of an attempt to inhibit competition rather than a serious effort to improve security.

Q. IS THERE ANY WAY THAT THE DEPARTMENT CAN DETERMINE WHETHER VERIZON'S PROPOSAL REFLECTS ANY REASONABLE WEIGHING OF COSTS AND BENEFITS?

A. Perhaps one way to think about the problem is to consider whether Verizon would propose such draconian and costly methods for solving relatively low level security risks if it had to bear all, or even its fair share of the costs. Indeed, if the Department were to make clear that all carriers have a joint interest in ensuring that the network is secure and,

therefore, that all carriers must share the cost responsibility in ratable manner reflecting their respective shares of telephone lines, Verizon's proposal might then reflect the sort of rational weighing of costs and benefits that must be done in order to come up with the right result. As long as Verizon, or indeed any carrier, can offer a security "wish list" without a need to balance other considerations, it is unlikely that it will provide a reasoned approach to the problem. This is especially true in this case, where Verizon proposes to impose all of the costs associated with its new security measures upon its competitors.

VI. CONCLUSIONS AND RECOMMENDATIONS.

Q. ARE THE COSTS ASSOCIATED WITH VERIZON'S PROPOSED COLLOCATION RULE CHANGES WARRANTED TO ADDRESS THE SECURITY RISKS IDENTIFIED, IN LIGHT OF THE ALTERNATIVE SECURITY MEASURES DESCRIBED?

A. It is very difficult to reach a final conclusion when Verizon has not specified precisely what it is proposing and therefore has not provided any estimate of the costs. Nevertheless, AT&T is confident that it makes little sense for the Department to adopt the costly and disruptive collocation measures proposed by Verizon. This is true because of the comparatively low level of risk of physical attack – a cyber or electronic attack remains the most likely mode of terrorism upon Massachusetts' telecommunications network. This is also true because of the demonstrated success of the security measures currently employed by AT&T. It would make little sense to adopt costly and disruptive collocation measures that would likely have little, if any incremental benefit.

Q. WHAT IS THE BASIC UNDERLYING PROBLEM WITH THE WAY THAT VERIZON HAS CONCEIVED THE PROBLEM?

A. Verizon simply assumes that access by only one company is necessary to achieve security – a convenient assumption when the one company with access is the dominant competitor in the market that can then restrict, preclude or make prohibitively expensive the access of all its rivals from their own equipment. Imagine if the dominant carrier at a major international airport were able to prevent all the other carriers from sharing use of the airport's facilities..

A major airport, in fact, is a useful counter-example. At an airport, the number of competing airlines and contractors with a need for access to equipment and facilities greatly exceeds the number of CLECs that might collocate at a Verizon central office. Concessions stands, restaurants, baggage handlers, news stands, catering companies delivering food to the airliners, ticket agents, and persons responsible for cleaning planes are just a few of the businesses and operational groups needing access to potentially sensitive areas at an airport. Obviously, no one suggests that the dominant airline – and no other company – should dictate the terms under which its competitors should have access to airport facilities. Moreover, given the substantially greater stake of airlines in security at airports, it would untenable for a dominant airline to impose greater restrictions upon its competitor's access to terminal facilities than would be imposed upon third parties with considerably smaller investments at potential risk. Clearly, the better approach is to recognize the common interest in optimizing security for all who share use of the airport. From this perspective, the key to security is good screening and tracking of the employees of all individuals whose employment requires them to be in secure portions of the airport. If such an approach is used at major airports, where the

potential for terrorists attack and the potential consequences are much greater than in a Verizon central office, there is no reason why such an approach cannot be adopted to protect Massachusetts' telecommunications network.

Q: PLEASE SUMMARIZE YOUR RECOMMENDATIONS.

A: We have four recommendations.

First, all telephone companies have a common stake in the security of the public telephone network from the risks of intentional, negligent, and accidental harm. Addressing these risks involves an analysis in which the magnitude of specific potential losses is weighed against the cost and likelihood of benefit of means to reducing the risks of such losses. Verizon's testimony does not appear to address the new risks of intentional harm made plain by the events of September 11, let alone weigh the costs of minimizing such risks against the possible benefits of such measures. Instead, Verizon's testimony appears to focus very narrowly upon the possible harm that may occur due to the presence of CLEC representatives in Verizon's central offices. Further, the harm discussed in the Verizon testimony appears to primarily address negligent and accidental harm that may be caused by such representatives. Verizon has not shown what the costs of its proposal would be, or whether the benefits of its proposal in terms of reduced risks would be worth the direct costs. Moreover, Verizon's proposal fails to address the fact that physical collocation provides considerable benefits to Massachusetts by making facilities-based competition more feasible and economic. Verizon's proposal would result in considerable harm to competition and the economy of Massachusetts. This real harm to the Commonwealth would exceed by far the theoretical risks that Verizon's panel has addressed. Thus, Verizon's proposal should be rejected by the Department.

Second, the presence of individuals in collocation central offices necessarily exposes all carriers with facilities in those locations to the risk that unqualified or unauthorized individuals may deliberately, negligently, or accidentally damage their facilities. The best means of confronting this risk is to adopt and implement a security system which, in a uniform and non-discriminatory manner, sets minimum standards of training, security clearance, and access protocols for anyone who seeks access to facilities in those central offices. These standards should be applicable, without any exception, to all carriers and there must be assurance that breaches of those standards will be detected promptly and reliably subject to financial and non-financial penalties. To the extent that the Department discovers that current procedures do not effectively create such uniform and non-discriminatory standards, it should explore the improvement of industry procedures in this proceeding.

Third, AT&T has a well-developed system for maintaining the security of its network facilities. Verizon's security system, and those of other carriers, may differ both from AT&T's and each others. All carriers and the public would benefit from the carriers sharing their practices in an effort to identify "best practices" that can be used at Verizon's collocation central offices to protect against terrorist and other harms to the facilities located at those offices. In analyzing these practices, the carriers' representatives should also consider the opinions of terrorism and law enforcement experts. Clearly, the best method of facilitating this type of productive exchange would be through the establishment of the industry task force that AT&T and other CLECs have already proposed to the Department

Fourth, the Department should eschew "change for change's sake." All changes of practices have cost to Verizon, its competitors, or both, that inevitably will flow through to customers. The Department should take into the account the likely benefit to the overall security of the public telephone network of any change against the cost that such a change will entail. If a change is deemed to be needed, it should be one which is best tailored to most effectively and affordably meet an identified risk in a competitively neutral manner. The Department must make measured and studied decisions concerning collocation security in order to insure that other critical telecommunications policy goals are not forfeited.

Q. DOES THAT CONCLUDE YOUR TESTIMONY?

A. Yes.

Attachment A (Proprietary Information)

Attachment B